CLAIMS

1. A common key generating method for generating a common key used in performing an encryption process of encrypting a plaintext into a ciphertext and a decryption process of decrypting the ciphertext into the plaintext mutually between a plurality of entities, comprising the steps of:

obtaining a secret key of one of the entities generated using identification information of the one entity; and

generating a common key based on the obtained secret key and identification information of the other entity as a communicating party,

wherein, if the identification information of the other entity lacks a component, the common key is generated after adding a part of components of the identification information of the one entity to the identification information of the other entity.

2. The common key generating method as set forth in claim 1, wherein

the identification information is an electronic mail address, and the part of components is a domain name.

3. A common key generator for generating a common key used in performing an encryption process of encrypting

a plaintext into a ciphertext and a decryption process of decrypting the ciphertext into the plaintext mutually between a plurality of entities, comprising

a controller capable of performing the following operations:

(i) obtaining a secret key of one of the entities generated using identification information of the one entity;

(ii) determining whether identification information of the other entity as a communicating party lacks a component; and

(iii) if it is determined that the identification information lacks a component, adding a part of components of the identification information of the one entity to the identification information of the other entity, and generating a common key based on the secret key of the one entity and the identification information of the other entity to which the part of components has been added.

4. The common key generator as set forth in claim 3, wherein

the identification information is an electronic mail address, and the part of components is a domain name.

5. A cryptographic communication method for transmitting information in ciphertext form between first

and second entities, comprising the steps of:

sending secret keys generated using identification information of the first and second entities from a key issuing agency to the respective entities;

at the first entity, if the identification information of the second entity lacks a component, adding a part of components of the identification information of the first entity to the identification information of the second entity, and generating a first common key based on the secret key of the first entity sent from the key issuing agency and the identification information of the second entity to which the part of components has been added;

at the first entity, encrypting a plaintext into a ciphertext by using the generated first common key, and transmitting the ciphertext to the second entity;

at the second entity, if the identification information of the first entity lacks a component, adding a part of components of the identification information of the second entity to the identification information of the first entity, and generating a second common key identical with the first common key, based on the secret key of the second entity sent from the key issuing agency and the identification information of the first entity to which the part of components has been added; and

at the second entity, decrypting the transmitted

ciphertext into a plaintext by using the generated second common key.

6. The cryptographic communication method as set forth in claim 5, wherein

the identification information is an electronic mail address, and the part of components is a domain name.

7. The cryptographic communication method as set forth in claim 5, wherein

a plurality of key issuing agencies are present, and each of the key issuing agencies generates secret keys of the first and second entities by using divided identification information obtained by dividing the respective identification information of the first and second entities.

8. A cryptographic communication system for performing an encryption process of encrypting a plaintext as information to be transmitted into a ciphertext and a decryption process of decrypting the transmitted ciphertext into the plaintext mutually between a plurality of entities, comprising:

a key issuing agency for issuing a secret key of each entity by using identification information of each entity; and

a plurality of entities, each of which generates a common key for use in the encryption process and decryption process based on its secret key issued by the key issuing agency and identification information of an entity as a communicating party,

wherein each of the entities is provided with a controller capable of performing the following operations:

(i) determining whether the identification information of the entity as the communicating party lacks a component; and

(ii) if it is determined that the identification information lacks a component, adding a part of components of its own identification information to the identification information of the entity, and generating a common key based on its secret key and the identification information to which the part of components has been added.

9. The cryptographic communication system as set forth in claim 8, wherein

the identification information is an electronic mail address, and the part of components is a domain name.

10. A computer memory product having computer readable program code means for causing a computer to

generate a common key used in performing an encryption process of encrypting a plaintext into a ciphertext and a decryption process of decrypting the ciphertext into the plaintext mutually between a plurality of entities, said computer readable program code means comprising:

program code means for causing the computer to obtain a secret key of one of the entities generated using identification information of the one entity;

program code means for causing the computer to determine whether identification information of the other entity as a communicating party lacks a component; and

program code means for causing the computer to add a part of components of the identification information of the one entity to the identification information of the other entity and to generate a common key based on the secret key of the one entity and the identification information of the other entity to which the part of components has been added, if the identification information of the other entity lacks a component.

11. A computer data signal embodied in a carrier wave for transmitting a program, the program being configured to cause a computer to generate a common key used in performing an encryption process of encrypting a plaintext into a ciphertext and a decryption process of

decrypting the ciphertext into the plaintext mutually between a plurality of entities, comprising:

a code segment for causing the computer to obtain a secret key of one of the entities generated using identification information of the one entity;

a code segment for causing the computer to determine whether identification information of the other entity as a communicating party lacks a component; and

a code segment for causing the computer to add a part of components of the identification information of the one entity to the identification information of the other entity and to generate a common key based on the secret key of the one entity and the identification information of the other entity to which the part of components has been added, if the identification information of the other entity lacks a component.